P2P Blockchain E-Voting System For The Masses

Saleh Jasim Al-Mukhattin

August 3, 2022

1 Introduction

In this White Paper, I aim to describe the system, it's advantages, it's limits, Solutions for expansion, and applications, In addition to that, I will scheme the engineering aspect of this project, to make it functional and safe as possible, I will further explain This scheme and it's characteristics.

2 Where did the idea come from

This is an idea that came to while I was sitting on my laptop, thinking about rules and regulations, things that are collectivly decided by people and made into moral rules on the internet without any platform of democracy, after that I thought, Why isn't there a platform where people can make rules(moral rules) about the internet and vote on them, since users are the main users of the platform(obviously), they should be given a platform where they decide what they see on it, and do on it. Furthermore, the thought of this expanded into more than just a regulation mechanism on the internet, into a reliable E-Voting system to the masses; if people are the users of 'something', they should decide what they see and do on this 'something', the 'something' can be a public place, a game, a discord server, etc, if you can replace the 'something' with something you see fit, then let it be a democracy for that 'something'.

2.1 Problems that I thought about

One problem that struck my mind instantly is that of the duplication of the votes, I asked my self then, how can I make the votes have scarcy, is there

a way that a number of vote for a number of rules be scarce for the number of people it was intended to?. Blockchain gives digital currency it's scarcy thus it's value;Blockchain will give the votes scarcy and thus value, is this enough?, no, because we need verification that one person is only one and not taking the place of other people, Here comes my Idea, but before that I need to introduce you to the scheme of the program. What will be the proof of the ledger, that a certain ledger is a valid ledger, bitcoin has proof of work, what can this voting system has, still not thought about it to be honest, it's a problem with a need of solution.

2.2 The Scheme

It's a blockchain network, There are 3 entities:

- Matters
- Rules
- Votes

Matters has Rules, Rules has Votes, Votes are by People. The Raiser raises a Matter with certain rules, those rules are uped or disuped, based on a certain function they are made into valid or not valid rules. A rule is validated every time a vote is made. Which means that it's a valid rule if enough people vote on it, this 'enough' is determined by a mathematical function, that I'm working on modeling. Whenever a Matter is opened, not everyone can make rules on it, there is a verification that has to be done, the raiser of the matter is the one to make the verification Through a platform he gives, the raiser decides how many Votes a person gets in this matter, the catch here is that the raiser doesn't decide how many each person give, he only decides the total number of votes for this matter; each person wil get an equal amount of votes, if he can prove he is a real person, but this way shouldn't reveal any information about the identity of that person, using a zero proof verifcation algorithm.

2.3 The Solution

A good verifcation method I thought of is, fingerprints, but not the exact fingerprint, a hashed fingerprint, a hashed version of it will be given to the verifier and one is available to the user on his finger(obviously), with a press of a finger, he will be able to verify and vote, knowing that the only way a person can steal his vote, is by cutting his finger or just stealing his finger hash.

Another Realistic method is that, After raising a matter and decided the targeted vote, The Raiser will put the contacts(Phone Numbers, ID's, anything that he can be sure belongs to one person) of the voters, random passcodes will be sent randomly to them, and they will be able to vote if they enter the passcode, this doesn't reveal the identity of a voter, only that they are valid.

Here the help of government authority is needed, for example public places, they have all the data of citizins, They can approve of this method of regulating and encourage people to respect those rules, It will help government establish a controlable democracy, even though it's a decentrilized, it's controlable by the matter raiser, in the way that the rules are not arbitary, they are decided by the raiser, they can discuss the raiser into adding new rules, but they are functionally just voters for a certain rule, unless the raiser is your friend.

2.4 The Program

The Network is different from the interface that the people will be able to raise and be verified and vote from, The interfaces are called clients, The Network is the server, though it's a typical P2P network, with no center, on the client side, the Raiser will raise a matter, with his account, and he chooses the participant, the client will have a method of sending emails or sms, taking hashes, the voters will join with their accounts, and will search for the matter, and put the verification method needed, then they will get their votes and will be able to see the rules and vote, once all people vote the matter will be closed.

2.5 Consensus Algorithm

Each Matter, will have it's consesus by the it's own members, the blockchain is built by merging the blockchains of each matter into one public big blockchain. So people will also decide about the ledger. This insures that the matter of a certain group people is decided by them and verified by them, unlike proof of stake and proof of work, this is a democratic way to handle consensus.